

JP2000174746A METHOD AND DEVICE FOR DECIPHERING DATA

Bibliography

DWPI Title

Data decoding method involves encrypting K pieces which are selected from divided secret key using disclosure key by preset specification which is stored in memory

Original Title

METHOD AND DEVICE FOR DECIPHERING DATA

Assignee/Applicant

Standardized: **HITACHI SOFTWARE ENG**

Original: HITACHI SOFTWARE ENG CO LTD

Inventor

SAMEJIMA YOSHIKI; MIYAZAKI HIROSHI; TODA JUNICHI

Publication Date (Kind Code)

2000-06-23 (A)

Application Number / Date

JP1999267988A / 1999-09-22

Priority Number / Date / Country

JP1998278012A / 1998-09-30 / JP

JP1999267988A / 1999-09-22 / JP

Abstract

PROBLEM TO BE SOLVED: To decipher data or file enciphered with a public key without knowing a secret key itself and to facilitate the management of divided keys as well by dividing the secret key with a stored primary expression and deciphering the data enciphered with the public key while using divided keys.

SOLUTION: A computer 101 enciphers and preserves a document or file prepared by a user. A key generating means 102 generates the key pair of cipher to be used for the users of plural user computers 101, namely, the public key and secret key of public key cipher. The generated key pair is sent to the user computer 101 and the secret key is divided and sent to divided key holding computers 103. N pieces of divided key holding computers 103 are installed, for example, and hold the divided secret keys of the user. A data deciphering device 104 extracts information concerning the desired enciphered document to be deciphered from the user computer 101 and collects partially deciphered information from K (K

(51) Int.Cl.⁷

H 0 4 L 9/08

G 0 9 C 1/00

識別記号

6 2 0

F I

H 0 4 L 9/00

G 0 9 C 1/00

H 0 4 L 9/00

テーマコード (参考)

6 0 1 A

6 2 0 Z

6 0 1 F

審査請求 有 請求項の数 6 O L (全 19 頁)

(21) 出願番号

特願平11-267988

(22) 出願日

平成11年9月22日 (1999.9.22)

(31) 優先権主張番号

特願平10-278012

(32) 優先日

平成10年9月30日 (1998.9.30)

(33) 優先権主張国

日本 (J P)

(71) 出願人 000233055

日立ソフトウェアエンジニアリング株式会
社

(72) 発明者 飯島 吉青

神奈川県横浜市中区尾上町 6 丁目 81 番地

神奈川県横浜市中区尾上町 6 丁目 81 番地
日立ソフトウェアエンジニアリング株式会
社内

(74) 代理人 100083552

弁理士 秋田 収喜

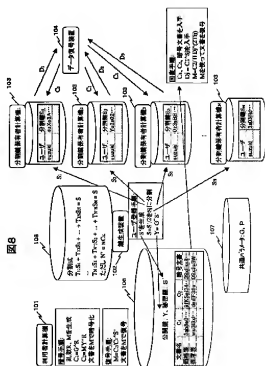
最終頁に続く

(54) 【発明の名称】 データ復号方法および装置

(57) 【要約】

【課題】 秘密鍵自体を知られることなく、複数人の分割鍵保有者の協力により、公開鍵で暗号化されたデータを復号でき、かつその分割鍵の管理も容易にする。

【解決手段】 公開鍵暗号の公開鍵と秘密鍵の鍵ペアのうち秘密鍵が N 個 ($N \geq 2$ の整数) に分割され、それぞれを N 人の分割鍵保有者に保有させ、 N 人のうち K ($K < N$) 人が保有する秘密鍵を用いて前記公開鍵で暗号化されたデータをコンピュータにより復号する場合に、前記分割鍵保有者の数 N に 1 を加えた数の変数を含む複数の一次式で、1 つの変数の係数は常に 0 でなく、残り N 個の変数の係数のうち K 個が 0 でない複数の一次式を利用して秘密鍵を N 個に分割し、その分割された N 個の秘密鍵のうち K 個を用いて前記公開鍵で暗号化したデータを復号する。



【特許請求の範囲】

【請求項1】 公開鍵暗号の公開鍵と秘密鍵の鍵ペアのうち秘密鍵をN個 ($N \geq 2$ の整数) に分割し、それぞれの分割鍵をN人の分割鍵保有者に割り当てた際の分割鍵保有者の数Nに1を加えた数の変数を含む複数の一次式で、かつ1つの変数の係数は常に0でなく、残りN個の変数における係数のうちK個が0でない複数の一次式を予め記憶した記憶手段を備え、前記N人のうちK ($K < N$) 人に割り当てた分割鍵を用いて前記公開鍵で暗号化されたデータをコンピュータにより復号するデータ復号方法であって、

前記秘密鍵を分割する際に、前記記憶手段に記憶された一次式を読み出し、該一次式によって前記秘密鍵をN個に分割し、その分割されたN個の分割鍵のうちK個を当該分割鍵の保有者から入力させて前記公開鍵で暗号化したデータを復号することを特徴とするデータ復号方法。

【請求項2】 請求項1記載のデータ復号方法において、前記秘密鍵を N_0 個 ($N \geq G \geq 2$ の整数) に分割し、それぞれの分割鍵をN人の分割鍵保有者をグループ化した N_0 個のグループに割り当て、さらにそれぞれのグループにおいて該分割鍵を各グループの所属人数 N_i 個 ($i \geq 1$ の整数) に分割し、それぞれを N_i 人の分割鍵保有者に割り当て、 N_i 人のうち K_i 人 ($N_i \geq K_i \geq 1$ の整数) の協力が成立した K_0 個のグループが協力して前記公開鍵で暗号化されたデータをコンピュータにより復号する場合において、

分割鍵保有者のグループ数 N_0 に1を加えた数の変数を含む複数の一次式で、1つの変数の係数は常に0でなく、残り N_0 個の変数の係数のうち K_0 個が0でない複数の一次式であり、さらに該残り N_0 個のそれぞれの変数は、その変数自身と N_i 個の変数を含む複数の一次式で表され、その変数自身の係数は0でない共通の値であり、残り N_i 個の変数の係数のうち K_i 個が0でない一次式を前記記憶手段に予め記憶させるステップと、前記秘密鍵を分割する際に、前記記憶手段に記憶された一次式を読み出し、該一次式によって前記秘密鍵を N_i 個に分割するステップと、

分割された N_i 個の秘密鍵のうち K_i 人が入力した K_0 個の秘密鍵を用いて前記公開鍵で暗号化したデータを復号するステップとを有することを特徴とするデータ復号方法。

【請求項3】 請求項2記載のデータ復号方法において、N人の分割鍵保有者のうち、協力が必須となる分割鍵保有者が N_A 人いる場合に、該必須分割鍵保有者を唯一の所属構成員とする N_A 個のグループと、残りの $N - N_A$ 人を所属者構成員としてそのうち $K - N_A$ 人の協力が必須となるグループに分け、さらにこれら $N_A + 1$ 個のグループ全部が協力して前記公開鍵で暗号化されたデータを復号する場合において、

前記 $N_A + 1$ 個のグループ全部が必要となる一次式を生成し、その生成した一次式を用いて前記秘密鍵を分割してN人の分割鍵保有者に割り当て、割り当てた秘密鍵を用いて前記公開鍵で暗号化したデータを復号することを特徴とするデータ復号方法。

【請求項4】 公開鍵暗号の公開鍵と秘密鍵の鍵ペアのうち秘密鍵をN個 ($N \geq 2$ の整数) に分割し、それぞれの分割鍵をN人の分割鍵保有者に割り当て、N人のうちK ($K < N$) 人に割り当てた分割鍵を用いて前記公開鍵で暗号化されたデータを復号するデータ復号装置であって、

前記分割鍵保有者の数Nに1を加えた数の変数を含む複数の一次式で、かつ1つの変数の係数は常に0でなく、残りN個の変数における係数のうちK個が0でない複数の一次式を予め記憶した記憶手段と、前記記憶手段に記憶された一次式を読み出し、該一次式によって前記秘密鍵をN個に分割し、その分割されたN個の分割鍵をN人の分割鍵保有者に割り当てる鍵生成手段と、

N人の分割鍵保有者に割り当てたN個の分割鍵のうちK個を当該分割鍵の保有者から入力させる入力手段と、入力されたK個の分割鍵を用いて前記公開鍵で暗号化したデータを復号する復号手段とを備えることを特徴とするデータ復号装置。

【請求項5】 暗号化されたデータの復号開始時に、復号に必要な分割鍵の数または分割鍵保有者数を表示する表示手段をさらに備えることを特徴とする請求項4記載のデータ復号装置。

【請求項6】 N人の分割鍵保有者に割り当てる分割鍵は、携帯可能な記録媒体に格納して各分割鍵保有者に保有させることを特徴とする請求項4または5記載のデータ復号装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、公開鍵暗号の公開鍵と秘密鍵の鍵ペアのうち秘密鍵をN個 ($N \geq 2$ の整数) に分割し、それぞれのN人の分割鍵保有者に保有させ、N人のうちK ($K < N$) 人が保有する秘密鍵を用いて前記公開鍵で暗号化されたデータをコンピュータにより復号するデータ復号方法および装置に関し、例えば、企業内で担当者が作成、暗号化した文書を、その担当者が不在の時に復号する必要が生じた場合に、担当者の上長や所属のコンピュータ管理者が協力し、あるいはさらに特定の誰かによる協力を受けて復号する場合のデータ復号方法および装置に関するものである。

【0002】

【従来の技術】 従来において、複数人の分割鍵保有者に預けた秘密鍵を用いて、該秘密鍵に対応する公開鍵で暗号化したデータを復号する方法として、Shamir (A. Shamir, "How to share a secret", Communication of ACM

22 (11)、612-613、1979年11月号)の方法がある。この方法では、秘密鍵の情報を N 人 ($N \geq 2$ の整数)の分割鍵保有者に分割して渡し、そのうち K 人 ($K \leq N$)が保有する分割鍵秘密鍵を集めることにより秘密鍵自体を復元し、その復元した秘密鍵によって、暗号化したデータを復号化可能にしたものである。

【0003】一方、暗号通信を不正目的に利用しているユーザの通信内容を解読して犯罪捜査に利用する方法として、暗号文の復号鍵を供託機関に登録しておいて、捜査が必要な場合に捜査機関が裁判所の許可を受け、復号鍵を供託機関から入手し、その入手した復号鍵によって暗号文を解読して捜査に利用する方法が提案されている。この時、供託機関自身の不正を防止するため、1つの供託機関にのみ復号鍵を供託するのではなく、複数の供託機関に分割して供託し、そのうち幾つかの供託機関が協力して、元の復号鍵を復元し、解読に利用する方法である。Micali (S. Micali, "Fair Public-Key Cryptosystems", Proceedings of Crypto' 92, 111-138)の方法がある。

【0004】また、機密データの漏洩を防ぐ手段の1つとして、例えば特開平8-446332公報「ファイル暗号装置」等のファイルを暗号化する方がこれまでにいくつか提案されている。暗号化したファイルは、そのファイルを暗号化したユーザだけが復号することができる。

【0005】【発明が解決しようとする課題】ところが、Shamirの方法では、 K 人が集まると、秘密鍵そのものが復元されてしまう。よって、その秘密鍵で復号可能な全てのデータを復号することができ、復号目的以外の必要以上の他の情報が K 人の人間に知られてしまう危険性がある。

【0006】一方、Micaliの方法では、組み合わせの数が大きくなると供託機関が持つ分割した復号鍵の数が大きくなるという問題があった。例えば、5つの供託機関があり、このうち3つが協力して鍵を持つとなると、機関Aは、BとC、BとD、BとE、CとD、CとE、DとE、という具合に協力機関の組み合わせ数だけ分割鍵を持つ必要があり、分割した復号鍵の管理が面倒で複雑化し、そのコストが嵩むという問題があった。

【0007】また、これらの方法では復号鍵の復元の際に特定の誰かを必須にしたり、分割鍵の所有者をグループ化してそれぞれのグループ内で協力が成立しないと復元できないようにする、といった柔軟な分割が行えなかった。

【0008】また、分割鍵保有者の変更の場合には、旧保有者の結託による不正な復号鍵の復元を防ぐために秘密鍵を分割し直す必要があるが、全員に再配布しなければならず影響範囲が大きい、という問題も起きてしまう。

【0009】さらに、特定の復号鍵を復元する際に、特

定の誰かを必須にすることは、上記の方法でも必須の分割鍵保有者に複数の分割鍵を割り当てることで実現できていたが、この場合でも分割鍵保有者の変更時には全員に再配布する必要があった。

【0010】さらに、ファイルを暗号化する場合については、特開平8-446332公報「ファイル暗号装置」等の装置では、暗号化ファイルを所有するユーザしかファイルを復号することができない。このため、企業内で担当者が作成した文書で、前記装置を用いて暗号化した場合、顧客や他部署などから前記文書に関する問い合わせがあったときに、前記担当者が不在の場合には前記文書を復号できないという問題があった。

【0011】さらに、前記公報に開示された「ファイル暗号装置」では、ファイルを復号する際にパスワードの入力を求められるが、パスワードを忘れてしまうとファイルを復号できないという問題もあった。

【0012】本発明の目的は、秘密鍵自体を知られることなく、複数人の分割鍵保有者の協力により、公開鍵で暗号化されたデータあるいはファイルを復号でき、かつその分割鍵の管理も容易であるデータ復号方法を提供することにある。

【0013】本発明の他の目的は、分割鍵を復元する際に特定の誰かが保有する分割鍵を必須の条件としたり、分割鍵の所有者をグループ化してそれぞれのグループ内で協力が成立しないと復元できないようにするなどの柔軟な分割を行い、その分割された鍵を用いて、暗号化されたデータを復号することができるデータ復号方法を提供することにある。

【0014】本発明のさらに他の目的は、複数人の分割鍵保有者の協力により、公開鍵で暗号化されたデータあるいはファイルを簡単な操作で容易に復号することができるデータ復号装置を提供することにある。

【0015】【課題を解決するための手段】上記目的を達成するために、本発明は、公開鍵暗号の公開鍵と秘密鍵の鍵ペアのうち秘密鍵を N 個 ($N \geq 2$ の整数)に分割し、それぞれの分割鍵を N 人の分割鍵保有者に割り当てた際の分割鍵保有者の数 N に1を加えた数の変数を含む複数の一次式で、かつ1つの変数の係数は常に0でなく、残り N 個の変数における係数のうち K 個が0でない複数の一次式を予め記憶した記憶手段を備え、前記 N 人のうち K ($K < N$)人に割り当てた分割鍵を用いて前記公開鍵で暗号化されたデータをコンピュータにより復号するデータ復号方法であって、前記秘密鍵を分割する際に、前記記憶手段に記憶された一次式を読み出し、該一次式によって前記秘密鍵を N 個に分割し、その分割された N 個の分割鍵のうち K 個を用いて前記公開鍵で暗号化したデータを復号することと特徴とする。

【0016】詳しくは、次に述べる $N+1$ 変数の一次式に基づいて秘密鍵を分割して分割鍵保有者に預ける。こ

のうちK人が集まれば、暗号化したデータが復号できるように構成し、秘密鍵そのものは復元されないように構成したものである。

【0017】説明のため、秘密鍵を S' 、 $S = S' / 2$ を「1」から「10」までのある整数とみなし、秘密鍵 S' を3人に分割して、2人が集まってデータを復号する場合を例に挙げると、まず、「位数11」の有限体 Z_{11} 上で以下の一次式を作成する。

【0018】

$$\text{【数1】 } 1S_1 + 1S_2 + 0S_3 = S \pmod{11}$$

【0019】

$$\text{【数2】 } 2S_1 + 0S_2 + 1S_3 = S \pmod{11}$$

【0020】

$$\text{【数3】 } 0S_1 + 2S_2 + 10S_3 = S \pmod{11}$$

ここで、数3は、数1の2倍から数2を引き算することによって得られることに注意する。すると、ある S_1 、 S_2 、 S_3 、 S についてある2つの式が成立すると、残りの式も成立することになる。公開鍵暗号としては、ある数のべき乗を求めることで復号する方式を選ぶ。

【0021】また、上記の分割鍵について同様な方法で一次式を作成し、さらに分割を繰り返すことで、分割鍵保有者をグループ化したそれぞれのグループ内での協力と、グループ単位での協力を組み合わせた復号を行うようにする。あるいは、グループ化の際にあるグループでは全員参加の協力とし、さらに全グループでの協力を必要とすることで、ある特定の分割鍵保有者の協力を必須とする条件で復号を行うようにする。

【0022】また、分割鍵保有者の変更時の課題を解決するため、分割鍵保有者をグループ化したそれぞれのグループ内での協力と、グループ単位での協力を組み合わせた復号を行えるよう、上記方法で秘密鍵を分割した後、分割鍵についても同様に一次式を作成してさらに分割を繰り返すように構成したものである。

【0023】さらに、本発明のデータ復号方法を適用したデータ復号プログラムをファイル暗号装置に実装し、前記データ復号プログラムのインタフェースを用いてデータあるいはファイルを暗号化する担当者の秘密鍵を分割し、その分割鍵を前記担当者の上長や所属のコンピュータ管理者に保有させ、暗号化操作を行った担当者が不在のときでも、前記データ復号プログラムを用いてコンピュータ管理者等の分割鍵保有者が協力して、暗号化されたデータあるいはファイルを復号できるように構成したものである。

【0024】

【発明の実施の形態】以下、図面に従い、本発明の実施の形態について説明する。図1は、本発明を適用した暗号データの復号システムの一実施形態を示すシステム構成図である。図1において、101は、一般の利用者が使う計算機であり、利用者の作成した文書あるいはファイルを暗号化して保管する。102は、鍵生成装置であ

り、複数の利用者計算機101の利用者が使用する暗号の鍵ペア、すなわち公開鍵暗号の公開鍵と秘密鍵を生成する。生成した鍵ペアは利用者計算機101に、また秘密鍵は分割して分割鍵保有者計算機103に送る。

【0025】103は分割鍵保有者計算機であり、利用者の分割された秘密鍵を保持している。ここでは、N台の分割鍵保有者計算機103が設置されているものと仮定する。

【0026】104はデータ復号装置であり、利用者計算機101から復号したい暗号化文書に関する情報を取り出し、K台（ $K < N$ ）の分割鍵保有者計算機103から部分的に復号された情報を集め、利用者が暗号化した文書を復号する。105は、利用者計算機101と鍵生成装置102とデータ復号装置104と分割鍵保有者計算機103とを接続するネットワークである。

【0027】以上の構成において、まず、システム構築時に鍵生成装置102において行う処理の概要を図2のフローチャートを参照して説明する。なお、ここで例示するビット数は、本出願時の暗号学により、ある程度の安全性が保証されている数であり、今後大きくないと予想される。また、秘密鍵の分割に必要な計算式等のアルゴリズムは、各計算式を必要とする計算機の内部の記憶装置に予め記憶され、必要の都度読み出されて使用されるものである。

【0028】まず、ステップ201において、暗号パラメータ p 、 G を生成する。暗号パラメータ p は、1024ビット以上の素数であり、この p と共に、 $p = 2q + 1$ なる q も素数になるように求める。そして、 p を法として位数 $p-1$ がとなる数 G （原始根）を求める。定義より G は、数4に示すように、 p を法として $p-1$ 乗して始めて「1」となる数である。

【0029】

$$\text{【数4】 } G_p \cdot q^{-1} = 1 \pmod{p}$$

次に、ステップ202において、 N 個から K 個を選択する組み合わせの数 C_K^N に等しい個数の恒等式 T_i を生成する。生成の方法は図3を用いて後述する。恒等式は Z_q で求める。ここで Z_q は「0」から「 $q-1$ 」までの整数からなる集合で q を法とした加減乗除の演算を行う。

【0030】次にステップ203において、前記ステップ201、202において得られた p 、 G を利用者計算機101と分割鍵保有者計算機103に送り、 p 、 G 、 T_i をデータ復号装置104に送る。

【0031】図3は、恒等式 T_i の生成方法を示すフローチャートである。なお、ここで分割鍵保有者の数を N 、復号に必要な分割鍵保有者の数を K とする。第1例では、 $N=3$ 、 $K=2$ 、 $p=23$ として、すなわち、3人の分割鍵保有者のうち、2人が協力して復号する場合を例に挙げて具体的に説明する。

【0032】まず、ステップ301、302において、変数 i 、 j の初期化を行い、 $i=1$ 、 $j=1$ とする。

【0033】次のステップ303, 304, 305において、恒等式 T_1 における S_2 の係数をランダムに定める。この結果、具体的には、 i が「1」の時、 T_1 について S_1 の係数が例えば「5」となる。

【0034】次のステップ306において、 S_2 と S の係数が「1」、 S_3 の係数が「0」となる。以上で T_1 が決定し、次の、数5の式となる。

【0035】

【数5】

$$5S_1 + 1S_2 + 0S_3 = S \pmod{11} \quad \cdots T_1$$

次に、ステップ307において、 i が「2」、 N が「3」、 K が「2」であるので、「 $i \leq N-K+1$ 」が成立して、 i を「2」に更新してステップ302、303、304の処理を同様に行い、 T_2 の S_j の係数を定める。この結果、具体的には、 S_1 の係数が例えば「8」となる。さらにステップ306において、 S_3 と S の係数が「1」、 S_2 が「0」となる。以上までで、 T_2 が定まり、次の、数6のようになる。

【0036】

【数6】

$$8S_1 + 0S_2 + 1S_3 = S \pmod{11} \quad \cdots T_2$$

次に、ステップ308において、 S_2 と S_3 の係数が「0」でない T_3 を求めるために、今まで求めた式で、 S_2 の係数が「0」でない式 T_1 と S_3 の係数が「0」でない式 T_2

$$7S_1 + 2S_2 + 1S_3 + 0S_4 + 0S_5 = S \pmod{11} \quad \cdots T_1$$

続くステップ307において、 i が「2」、 N が

「5」、 K が「3」であるので、「 $i \leq N-K+1$ 」が成立して、 i を「2」に更新してステップ302、303、304の処理を行い、 T_2 の S_j の係数を定める。例

$$3S_1 + 5S_2 + 0S_3 + 1S_4 + 0S_5 = S \pmod{11} \quad \cdots T_2$$

同様に T_3 式が例えば、以下の、数11のようになる。

【0044】

$$10S_1 + 3S_2 + 0S_3 + 0S_4 + 1S_5 = S \pmod{11} \quad \cdots T_3$$

以下、同様にしてステップ308からステップ311で残りの式を求める。

【0045】5人の分割鍵保有者から3人を選ぶ残りの組み合わせは、(1, 3, 4)、(1, 3, 5)、(1, 4, 5)、(2, 3, 4)、(2, 3, 5)、(2, 4, 5)、(3, 4, 5)の7つの組み合わせがある。以下、残りの式を先の3つの式から求める。

(1, 3, 4)に対応する T_4 を求めるには、 S_3 の係数が「0」でない T_1 と S_4 の係数が「0」でない T_2 から計

$$6S_1 + 0S_2 + 9S_3 + 3S_4 + 0S_5 = S \pmod{11} \quad \cdots T_4$$

となる。

【0048】以下同様にして、 T_5 、 T_6 、 T_7 、 T_8 、 T_9 、 T_{10} を求める。以下のようになる。

$$1S_1 + 0S_2 + 3S_3 + 0S_4 + 9S_5 = S \pmod{11} \quad \cdots T_5$$

$$4S_1 + 0S_2 + 0S_3 + 7S_4 + 3S_5 = S \pmod{11} \quad \cdots T_6$$

$$0S_1 + 10S_2 + 2S_3 + 10S_4 + 0S_5 = S \pmod{11} \quad \cdots T_7$$

$$0S_1 + 7S_2 + 7S_3 + 0S_4 + 5S_5 = S \pmod{11} \quad \cdots T_8$$

とを選択する。

【0037】次に、ステップ309において、 T_3 は S_1 の係数が不要、つまり「0」になるように T_1 と T_2 から計算する。具体的には T_1 を8倍したもののから5倍した T_2 を引いて T_3 を次の、数7、数8を計算して得る。

【0038】

$$\text{【数7】 } 0S_1 + 8S_2 + 6S_3 = 3S \pmod{11}$$

【0039】

【数8】両辺を3で割って

$$0S_1 + 10S_2 + 2S_3 = S \pmod{11} \quad \cdots T_3$$

以上において法(mod)を「11」として計算していることに注意する。

【0040】別の例として、分割鍵保有者が5人で、このうち3人が協力する場合の例を挙げる。この場合、 $N=5$ 、 $K=3$ となる。

【0041】まず、ステップ303、304、305において、 T_1 の S_j の係数を定める。具体的には、 i が「1」の時、 T_1 について S_1 の係数が例えば「7」、 S_2 の係数が例えば「2」となる。さらにステップ306において S_3 と S の係数が「1」、 S_4 と S_5 の係数が「0」となる。 T_1 は次の、数9の通りとなる。

【0042】

【数9】

例えば、次の、数10のように T_2 が決まる。

【0043】

【数10】

$$3S_1 + 5S_2 + 0S_3 + 1S_4 + 0S_5 = S \pmod{11} \quad \cdots T_2$$

【数11】

算する。この時、 S_2 の係数が不要となるので、 T_1 と T_2 で S_2 の係数を消去するように計算する。具体的には、5倍の T_1 式から2倍の T_2 式を引くと以下の T_4 が求まる。

【0046】

【数12】

$$7S_1 + 0S_2 + 5S_3 + 9S_4 + 0S_5 = 3S \pmod{11}$$

【0047】

【数13】両辺を3で割って、

$$2S_1 + 0S_2 + 5S_3 + 3S_4 + 0S_5 = S \pmod{11} \quad \cdots T_4$$

【0049】

【数14】

$$0S_1 + 9S_2 + 0S_3 + 3S_4 + 9S_5 = S \pmod{11} \quad \cdots T_9$$

$$0S_1 + 0S_2 + 4S_3 + 6S_4 + 2S_5 = S \pmod{11} \quad \cdots T_{10}$$

最後の T_{10} 式は、上の式を用いて計算する。例えば、 S_1 と S_3 と S_4 の係数が「0」でない T_4 と S_1 と S_3 と S_5 の係数が「0」でない T_6 から S_1 の係数を消去して得ることができる。

【0050】ステップ309の消去の過程で、必要な係数まで消去される場合がある。ここで必要な係数とは S や上記の T_{10} でいえば S_3 、 S_4 、 S_5 の係数である。例えば、 N が「3」、 K が「2」の場合で、 T_1 と T_2 式が以下になったとする。

【0051】

$$\text{【数15】 } 1S_1 + 1S_2 + 0S_3 = S \pmod{11}$$

【0052】

$$\text{【数16】 } 1S_1 + 0S_2 + 1S_3 = S \pmod{11}$$

S_1 を消去するため、数15から数16を引くと

【0053】

$$\text{【数17】 } 0S_1 + 1S_2 + 10S_3 = 0S \pmod{11}$$

となり、 S の係数が「0」となり、必要な係数が消えている。このような場合は、最初からやり直す。

【0054】次に、図4を用いて鍵生成装置102にて行う利用者の登録方法を説明する。図4において、先ずステップ401において、秘密鍵 S' を「1」以上「 $p-1$ 」未満の偶数、ここでの例の場合「1」から「2」の数からランダムに選ぶ。ここでは「12」と仮定する。さらに S を秘密鍵 S' の半分の「6」とする。

【0055】次にステップ402において、秘密鍵 S を分割して S_1 を求める。ここでは先に求めた一次式を利用して分割秘密鍵 S_j を計算する。この分割秘密鍵 S_j を計算するための一次式は、鍵生成装置102の記憶装置に予め記憶されているものである。

【0056】

$$\text{【数18】 } 5S_1 + 1S_2 + 0S_3 = S \pmod{11}$$

【0057】

$$\text{【数19】 } 8S_1 + 0S_2 + 1S_3 = S \pmod{11}$$

【0058】

$$\text{【数20】 } 0S_1 + 10S_2 + 2S_3 = S \pmod{11}$$

S_1 をランダムに定める。すると、数18より S_2 が、数19より S_3 が求まる。例えば、 $S_1 = 3$ とすると、 $S_2 = 2$ 、 $S_3 = 4$ と分割できる。これは数20を満たしている。

【0059】次にステップ403において、この S_1 、 S_2 、 S_3 をそれぞれの分割鍵保有者計算機103に分割秘密鍵の内容が他に分からないように送る。送る方法には幾つかあるが、本発明の範囲外であるのでその説明は省略する。

【0060】次に、ステップ404において、秘密鍵 S' と公開鍵 Y を利用者計算機101に登録する。この場合の公開鍵 Y は、数21で表される。

【0061】

【数21】

【数21】

【0062】次に、登録の終了後、利用者が計算機101を用いて、自分が作成した文書を暗号化する方法について図5のフローチャートを用いて説明する。まず、ステップ501において、乱数 R と M を生成する。次に、ステップ502において、数22を計算する。

【0063】

【数22】

【数22】

$$C_1 = G^R$$

$$C_2 = M \cdot Y^R$$

【0064】ここで Y は、ステップ404で登録した利用者の公開鍵であり、計算は p を法として、ここでは「23」で計算する。

【0065】次のステップ503において、 M を秘密鍵暗号の鍵とみなして文書を暗号化する。見なしかたは本発明の範囲外であるので省略する。また、暗号方法には、公開鍵暗号に比べて高速な秘密鍵暗号を用いる。この暗号方法についても本発明の対象外であるので、省略する。続くステップ504において、 C_1 、 C_2 、 M で暗号化した文書を保管する。

【0066】次に、利用者計算機101を用いて暗号化された文書を復号する手順を図6のフローチャートにより説明する。復号する場合、まず、ステップ601において、数23を計算して、 M を求める。

【0067】

【数23】

【数23】

【0068】次に、数23から M を求める。この M を秘密鍵暗号の鍵とみなして暗号化した文書を復号する。

【0069】次に、暗号化した文書をデータ復号装置104にて復号する手順を図7のフローチャートを用いて説明する。まず、ステップ701において、復号したい文書と対応する C_1 と C_2 とを利用者計算機101から取り出す。

【0070】次に、ステップ702において、 K 個の利用する分割鍵保有者計算機103を選択し、その計算機103との安全な通信路を確立する。選択と安全な通信路の確立に付いては、本発明の範囲外であるので省略する。

【0071】次にステップ703において、上記通信路を使って、 C_1 を分割鍵保有者計算機103に送る。そして、ステップ704において、各分割鍵保有者計算機103が計算した部分復号結果 D_j を受け取る。この D_j は、数24で表される。

【0072】

【数24】

【数24】

【0073】次に、ステップ705において、数25を計算し、平文Mを得る。

【0074】

【数25】

【数25】

【0075】ここで $T_{1,j}$ は分割鍵保有者計算機103を選んだかによって決まる。先の恒等式を用いて、具

【数27】

$$\begin{aligned} G / (D_1^{2732} \times D_2^{123}) &= H Y^2 / D_1^{20} D_2^4 = H Y^2 / C_1^{202} C_2^{43} \\ &= H G^{258} / C_1^{202+433} = H G^{258} / C_1^{635} = H \end{aligned}$$

【0078】次に、ステップ706において、Mを使って、暗号化した文書を復号する。図8は、以上の処理全体を分かり易くまとめたものであり、利用者計算機101の記憶手段106に格納された「価格表」と「在庫表」の暗号文書をデータ復号装置104で復号する例を示している。なお、図中のパラメータは上記の説明と同じである。また、共通パラメータG、pは、各計算機の記憶手段107に記憶されるようになっている。また、秘密鍵の分割式は鍵生成装置102の記憶手段108に予め記憶されるようになっている。

【0079】上記説明では、複数の分割鍵保有者計算機103に分割秘密鍵を保有させる例を説明したが、本発明は複数の鍵供託機関に供託しておく場合に同様に適用することができる。以下、図9を用いて、本発明を鍵供託に用いた場合を簡単に説明する。

【0080】図9において、110は受信者計算機、111は送信者計算機、112-1~112-Nは複数の供託機関計算機、113は鍵生成装置、114は公開鍵配布機関計算機、115は検索機関における計算機である。

【0081】ユーザ登録の際は、鍵を生成した後、公開鍵Yは公開鍵配布機関計算機114に送信し、秘密鍵S'は利用者に送る。

【0082】暗号文を送りたい送信者計算機111の送信者は、受信者計算機110の受信者の公開鍵Yを公開鍵配布機関計算機114から入手し、先の例と同じ方法で暗号化して、C₁とC₂と暗号化した文書を受信者計算機110に送る。受信者計算機110の受信者は、先の例と同じようにして文書を復号する。

【0083】犯罪の疑いがある場合は、捜査機関の計算機115の担当者は送信者計算機111から受信者計算機110への通信文を盗聴して、C₁とC₂と暗号化した文書を手する。解読の手順は回復の手順と同じである。

【0084】以上のように、本実施形態によれば、暗号

体的に説明すると、選んだ分割鍵保有者計算機103に対応する係数が「0」でない式を選び、その式のS_jの係数をT_{1,j}とする。例えば、2番目と3番目の分割鍵保有者計算機103を選んだとすると、次の、数26を選択する。

【0076】

【数26】 $0S_1 + 10S_2 + 2S_3 = S \pmod{11}$

すると、T₃₁ = 0、T₃₂ = 10、T₃₃ = 2となる。

すると、数27を計算することで、Mが得られる。

【0077】

【数27】

文を復号する際には秘密鍵そのものはどこにも復元されず、分割鍵保有者計算機103が持つ分割鍵S_jに基づいて部分的に復号したデータD_iを使って必要な文書を復号しているため、同じ鍵を用いて、暗号化した他の文書を復号することはできない。

【0085】また、秘密鍵自体を知られることもない。そして、複数人の分割鍵保有者の協力により、公開鍵で暗号化されたデータを目的とする暗号文のみに限って復号することができ、かつその分割鍵の管理も容易である。

【0086】次に、本発明の第2の実施形態について説明する。この第2の実施形態は、N人の分割鍵保有者をN₀個の複数のグループに分け、そのうちのK₀個 (K₀ < N₀) のグループにおいて、それらのグループに所属するN₀人 (N₀ ≥ 2の整数) うちK₀人 (K₀ < N₀) が協力してデータを復号する場合の方法に関するものである。なお、システム構成は図1と同じであり、以下では、図1のシステム構成を前提にして本実施形態における秘密鍵のグループ分割方法と、分割鍵によるデータの復号方法について説明する。

【0087】まず、本実施形態における秘密鍵のグループ分割方法において、システム構築時において鍵生成装置102で行う処理の概要について図10のフローチャートを参照して説明する。

【0088】まず、ステップ1001において、図2のステップ201と同様にして暗号パラメータp、q、Gを求める。

【0089】次に、ステップ1002において、図2のステップ202と同様にして、N₀個からK₀個を選択する組み合わせの数N_{CK0}に等しい個数の一次式T_{0i}を生成する(a=1,2,...,N_{CK0})。また、ステップ202と同様にしてN₀個からK₀個を選択する組み合わせの数に等しい個数の一次式T_{0i}を生成する(g=1,2,...,N₀)。これは、図3と同様の手順で生成するが、詳細は図11にて説明す

る。

【0090】次にステップ1003において、図2のステップ203と同様に、前記ステップ1001、1002において得られた暗号パラメータ p 、 q 、 G を利用者計算機101と分割鍵保有者計算機103に送り、 p 、 G 、 T_n 、 T_{g+1} をデータ復号装置104に送る。

【0091】図11は、恒等式 T_n 、 T_{g+1} の生成方法を示すフローチャートである。なお、ここでは、 $N=4$ 、 $N_0=2$ 、 $K_0=2$ 、 $N_1=1$ 、 $K_1=1$ 、 $N_2=3$ 、 $K_2=2$ 、 $p=23$ とする。

【0092】これは、A、B、C、Dの4人のうち3人が協力し、かつAが必須となるように秘密鍵を分割するのに相当するグループ分けである。すなわち、図14(a)に示すように、グループ1のメンバーはAのみ、グループ2のメンバーはB、C、Dの3人といったグループ分けである。

【0093】まず、ステップ1101において、 N_0 が2、 K_0 が2の場合における恒等式 T_n の変数 S_g の係数を定める。その方法は図3と同じである。ここでは、例えば次のような恒等式 T_1 が得られたとする。

【0094】

【数28】 $2S_1 + S_2 = S \pmod{11}$

次に、ステップ1102において、変数 g の初期化を行い、 $g=1$ とする。次に、ステップ1103において、 N_1 個から K_1 個を選択する組み合わせの数に等しい個数の一次式 T_{11} を生成する。ここでは N_1 が1、 K_1 が1であるため、例えば次のような恒等式 T_{11} が得られたとする。

【0095】

【数29】 $3S_{11} = S_1 \pmod{11}$

次に、ステップ1104において、 $g=g+1$ に更新した後、次のステップ1105で $g \leq N_0$ かを判定する。ここでは、 g が2であるので、ステップ1103に戻る。ステップ1103では、 N_2 個から K_2 個を選択する組み合わせの数に等しい個数の一次式 T_{21} を生成する。ここでは $N_2=3$ 、 $K_2=2$ であるため、例えば次のような恒等式 T_{21} が得られる。

【0096】

【数30】 $5S_{21} + 1S_{22} + 0S_{23} = S_2 \pmod{11}$

$8S_{21} + 0S_{22} + 1S_{23} = S_2 \pmod{11}$

$0S_{21} + 10S_{22} + 2S_{23} = S_2 \pmod{11}$

続くステップ1104、1105の処理を行うことにより、 $g=3$ となり、図11の処理を終える。

【0097】次に、図12を用いて、鍵生成装置102にて行う利用者の登録方法を説明する。まず、ステップ1201において、図4のステップ401と同様に、秘密鍵 S' とその半分の値 S を求める。次に、ステップ1202において、 T_n を使って S を分割し S_g を求める。この場合の求め方は、図4のステップ402と同様に、 S_1 をランダムに定めてから S_2 を計算する。ここで得られた S_1 はグループ1に、 S_2 はグループ2に割り当てるものとす

る。

【0098】次にステップ1203において、 $g=1$ に設定し、次のステップ1204において T_{g1} に合わせて各 S_g を分割し S_{g1} を求める。求め方は図4のステップ402と同様である。続いて、 $g \leq N_0$ かを判定し、YESならばステップ1203に戻って同様の処理を繰り返し、 T_{g1} に合わせて各 S_g を分割し S_{g1} を求める。次に、ステップ1207において、分割した鍵 S_{g1} を分割鍵利用者計算機103 $_{g1}$ に秘密裏に送って登録する。

【0099】ここでは、図14(a)に示すように、 S_{11} を分割鍵保有者Aが利用する分割鍵保有計算機103 $_{11}$ に、 S_{21} 、 S_{22} 、 S_{23} を分割鍵保有者B、C、Dが利用する分割鍵保有計算機103 $_{21}$ 、103 $_{22}$ 、103 $_{23}$ に配布して登録する。

【0100】最後に、ステップ1208において、図4のステップ404と同様に、秘密鍵 S' と公開鍵 $Y=G_{S'}$ を利用者計算機101に送る。

【0101】利用者計算機101では、鍵生成装置102から配付された秘密鍵 S' と公開鍵 $Y=G_{S'}$ を用いて文書やファイルの暗号化、および復号を行う。

【0102】次に、図13のフローチャートを用いて、暗号化した文書を、各分割鍵保有者が利用する各分割鍵保有計算機103 $_{11}$ 、103 $_{21}$ 、103 $_{22}$ 、103 $_{23}$ との協同作業によってデータ復号装置104にて復号する手順について説明する。

【0103】まず、ステップ1301において図7のステップ701と同様に、復号したい文書と対応する C_1 と C_2 とを利用者計算機101から取り出す。

【0104】次に、ステップ1302において、 N_0 個のグループの中から選んだ K_0 個の各グループについて、 K_0 個の分割鍵保有者計算機103を選択し、図7のステップ702と同様にその計算機との安全な通信路を確立する。

【0105】ここではグループ1の分割鍵保有者Aが使用する分割鍵保有計算機103 $_{11}$ 、グループ2の分割鍵保有者C、Dが使用する分割鍵保有計算機103 $_{22}$ 、103 $_{23}$ を選んだものとする。

【0106】次に、ステップ1303において、図7のステップ703と同様に、上記通信路を使って C_1 を分割鍵保有者計算機103 $_{11}$ 、103 $_{22}$ 、103 $_{23}$ に送る。

【0107】次に、ステップ1304において図7のステップ704と同様に、これらの分割鍵保有者計算機上で計算した部分解説結果 D_{k1} を受け取る。この部分解説結果 D_{k1} は、次の数31で表される。

【0108】

【数31】

【数31】

$$D_{k1} = C_1^{1/2d} \pmod{23}$$

【0109】次に、ステップ1305において図7の

ステップ705と同様な計算を行うことにより、平文Mを得る。この平文Mは、次の、数32で表される。

【0110】

【数32】

【数32】

【0111】ここで、 $N_{ng} = G_{ng} / \Pi_{ng} D_{ng}^{2 \times t_{11} + t_{12}}$ を選んだかによって決まる。恒等式 T_{ng} から、選んだグループに対応する係数が0でない式を選び、その式の S_{ng} の係数を t_{ng} とする。ここでは T_{ng} は次の、数33に示す T_1 ただ1つしかなく、 t_{11} は2、 t_{12} は1となる。

【0112】

【数33】 $2S_1 + S_2 = S \pmod{11}$

また、 t_{g1} はどの分割鍵保有者計算機103_{g1}を選んだかによって決まる。各グループについて、そのグループ

【数36】

$$\begin{aligned} C_1 / (D_1^{2 \times t_{11} + t_{12}} \times D_{22}^{2 \times t_{22} + t_{23}} \times D_{23}^{2 \times t_{23} + t_{22}}) \\ = NY_1 / D_1^{12} D_{22}^{22} D_{23}^4 = NY_1 / C_1^{12 \times 1} C_2^{22 \times 1} C_3^{4 \times 2} \\ = NG^{12 \times 1} / C_1^{12 \times (3 \times 1) + 1 \times (10 \times 2 + 2 \times 2)} = NG^{12 \times 1} / C_1^{2 \times (2 \times 1 + 2 \times 2)} \\ = NG^{12 \times 1} / C_1^{12} = NG^{12 \times 1} / G^{12} = M \end{aligned}$$

【0116】を計算することで、平文Mが得られる。このようにして平文Mが得られたならば、ステップ1306において、Mを使って暗号化した文書を復号する。

【0117】以上のように秘密鍵を分割することにより、暗号文の復号に際しては、ユーザAの協力が必要となる復号形を実現することができる。

【0118】なお、図14(a)において、「2/2に分割」、「1/1に分割」、「2/3に分割」とは、分割数と必須となる分割鍵の数を表すものであり、分母が分割数、分子が必須となる分割鍵の数を示している。図14(a)のような分割を行った場合に、 S_{11} の保有者が変わったとしても、 S_1 を図3の方法を使って S'_{11} を生成し、新たな保有者に配ればよい。同様に S_{21} 、 S_{22} 、 S_{23} のいずれかの保有者が変わっても、 S_2 を分割し直してそのグループ内で配布し直せばよい。あるいはグループ内で S_2 を分割する条件を変えてもその影響範囲はそのグループ内に限ることができる。

【0119】なお、本発明は図14(a)に示すような分割の仕方に限らず、同図14(b)に示すような様々な分割の仕方を行うことができる。

【0120】次に、本発明の第3の実施形態について説明する。この第3の実施形態は、1つの利用者計算機内で上述した方法によって秘密鍵を複数に分割し、各分割鍵を別々の利用者に割り当てておき、暗号文を復号する際に分割鍵の保有者の全部または必須とされる分割鍵の保有者の協力により、暗号文を復号するようにしたものであり、特に、復号する際のインタフェースの構成に関するものである。

【0121】図15は、第3の実施形態のシステム構成

に対応する恒等式 T_{gi} から、選んだ分割鍵保有者計算機103に対応する係数が0でない式を選び、その式の S_{gi} の係数を t_{gi} とする。ここでは、1つ目のグループについては次の、数34に示す恒等式 T_{11}

【0113】

【数34】 $3S_{11} = S_1 \pmod{11}$

から、 $t_{111} = 3$ となる。2つ目のグループについては、例えば2番目と3番目の計算機103₂₂、103₂₃を選んだとすると、次の、数35に示す恒等式 T_{23}

【0114】

【数35】 $0S_{21} + 10S_{22} + 2S_{23} = S_2 \pmod{11}$

から、 $t_{232} = 10$ 、 $t_{233} = 2$ となる。すると、

【0115】

【数36】

を示す図であり、1500は一般の利用者が使う計算機(利用者計算機)であり、中央処理部1501、入出力部1502、表示部1503、ファイル暗号部1504、鍵生成部1505、ファイル復号部1506から構成される。この利用者計算機1500は、例えばパーソナルコンピュータ等の汎用の計算機で構成することができる。

【0122】中央処理部1501は、システム構築、恒等式の作成、ユーザ登録、ファイル暗号、ファイル復号、入出力、表示などの一連の処理を制御する。

【0123】入出力部1502は、復号したいファイルあるいはデータの名前を入力したり、分割鍵を入出力したりするためのものである。この入出力部1502には、キーボード、マウス、フロッピーディスクドライブなどが用いられる。

【0124】表示部1503は、ファイル復号などの案内画面を表示するためのものである。この表示部1503には、ディスプレイなどが用いられる。

【0125】ファイル暗号部1504は、利用者の作成した文書を暗号化して図示しない記憶装置に保管する部分であり、図1の利用者計算機101と同様の機能を有する。

【0126】鍵生成部1505は、図1の鍵生成装置102と同様の機能を有するものであり、利用者が使用する暗号の鍵ペア、すなわち公開鍵暗号の公開鍵と秘密鍵を生成する。生成した鍵ペアはファイル暗号部1504に、また秘密鍵は分割して入出力部1502に送る。

【0127】ファイル復号部1406は、図1のデータ復号装置104と同様の機能を有するものであり、ファ

イル暗号部1504から復号したい暗号化ファイルに関する情報を取り出し、K個の分割鍵を集め、いずれかの利用者が暗号化したファイルを復号する。

【0128】前述の第1の実施例では、システムを構成する各装置がネットワーク105で接続されているが、本実施形態では、システムを構成する各部はすべて利用者計算機1500内にあり、ファイル復号に関する一連の処理はすべて利用者計算機1500内で行われる。

【0129】図16のフローチャートを用いて、システム構築時に行う処理の概要を説明する。まず、ステップ1601において、図2のステップ201と同様にして暗号パラメータp、q、Gを求める。次に、ステップ1602において、図2のステップ202と同様にして恒等式 T_1 を生成する。生成の方法は図3と同様である。

【0130】続く、ステップ1603において、暗号パラメータp、Gをファイル暗号部1504に、p、G、 T_1 をファイル復号部1506に送る。

【0131】図17は、鍵生成部1506にて行う利用者の登録方法を示すフローチャートである。まず、ステップ1701において、図4のステップ401と同様にしてSを選ぶ。次に、ステップ1702において、図4のステップ402と同様にして分割鍵 S_j を求める。次に、ステップ1703において、各 S_j に対して、分割鍵保有者認証情報 I_j を付加する。 I_j は、分割鍵保有者のID、パスワードなどの情報から構成されており、中央処理部1501が管理する。

【0132】次に、ステップ1704において、分割した鍵 S_j を出力部1502に出力し、認証情報 I_j を表示部1503に表示する。出力された分割鍵 S_j は、フロッピーディスクやICカード等の携帯可能な記録媒体に格納し、各分割鍵保有者が安全な場所に保管する。表示された認証情報 I_j は、各分割鍵保有者が他人に漏らさないように記憶しておくようにする。

【0133】次に、ステップ1705において、図4のステップ404と同様にして秘密鍵 S とYをファイル暗号部1504に登録する。

【0134】なお、本実施形態では、分割鍵 S_j を各分割鍵保有者が安全に管理することを要求しているが、分割鍵 S_j が入ったフロッピーディスク等の記録媒体の盗難などに対応するために、分割鍵 S_j を記録媒体に格納する際に、パスワードで暗号化している図18で説明する分割鍵保有者認証の際に分割鍵 S_j を復号するようにしてもよい。

【0135】次に、図18を用いて、複数の分割鍵保有者が協力して、利用者が暗号化したファイルを復号する手順を示す。なお、利用者がファイルを暗号化する方法と、利用者が自身が暗号化されたファイルを復号する手順は、それぞれ図5、図6と同様である。

【0136】まず最初に、ファイル復号に必要な人数の分割鍵保有者に、各自の分割鍵が格納された記録媒体を

持って集合してもらう。この状態で、ステップ1801において、分割鍵保有者の代表者または利用者計算機1500の管理者が、ファイル復号部1506を起動する。このファイル復号部1506やファイル暗号部1504および鍵生成部1505は、具体的には、ファイル復号プログラム、ファイル暗号プログラム、鍵生成部プログラムによって構成されるものである。

【0137】ファイル復号部1504が起動すると、中央処理部1501はステップ1802において、表示部1503にファイル復号情報を表示する。図19は、ファイル復号情報の画面表示例であり、分割鍵保有者の登録人数「3」と、ファイル復号に必要な分割鍵保有者の人数「2」が表示されている。

【0138】ファイル復号情報が表示されると、1人目の分割鍵保有者は、図19中の「OK」ボタンをクリックする。1人目の分割鍵保有者が「OK」ボタンをクリックすると、中央処理部1501は、ステップ1803において、表示部1503に分割鍵保有者認証画面を表示する。図20は、分割鍵保有者認証画面の表示例である。なお、ステップ1803において、分割鍵保有者が図20中の「キャンセル」ボタンをクリックした場合は、ファイル復号処理が中止される。本実施形態では、「キャンセル」ボタンが表示されている画面で、分割鍵保有者が「キャンセル」ボタンをクリックすると、ファイル復号処理を中止することができる。

【0139】分割鍵保有者認証画面が表示されると、ステップ1804において、分割鍵保有者は、分割鍵 S_j が格納された記録媒体を挿入し、ID、パスワードからなる認証情報を入力した後、図20中の「OK」ボタンをクリックする。

【0140】「OK」ボタンがクリックされると、中央処理部1501は、入力された認証情報と自身が管理している認証情報 I_j とを照合し、1人目の分割鍵保有者の認証を行う。なお、本実施形態では、分割鍵保有者の認証にパスワードを用いているが、分割鍵保有者の認証には、例えば指紋などによる他の認証方法を用いてもよい。

【0141】次に、中央処理部1501は、ステップ1705において、分割鍵保有者の必要な人数分の認証を行ったかどうかをチェックする。必要人数に達していない場合は、ステップ1803に戻って、分割鍵 S_j の入力および分割鍵保有者の認証を繰り返す。

【0142】必要人数に達した場合は、中央処理部1501は、ステップ1806において、表示部1503にファイル・保存先入力画面を表示する。図21は、ファイル・保存先入力画面の表示例である。

【0143】ファイル・保存先入力画面が表示されると、分割鍵保有者は、復号したいファイルの名前を入力するか、または図21中の上段の「参照」ボタン2101をクリックし、復号したいファイルの場所を参照す

る。

【0144】分割鍵保有者が「参照」ボタン2101をクリックすると、ステップ1807において、中央処理部1501は、表示部1503にファイル参照画面を表示する。図22は、ファイル参照画面の表示例である。

【0145】ファイル参照画面が表示されると、分割鍵保有者は、前記ファイル参照画面から復号したいファイルを選択する。例えば「readme. txt」を選択する。

【0146】ステップ1806で分割鍵保有者がファイルの名前を入力するか、またはステップ1807で分割鍵保有者がファイルを選択すると、ステップ1808において、中央処理部1501は、表示部1503にファイル・保存先入力画面を再び表示する。図23は、ファイル・保存先入力画面の表示例である。復号したいファイルの名前と、ファイル復号後の保存先が表示されている。

【0147】ファイル・保存先入力画面が表示されると、ステップ1809において、分割鍵保有者は、保存先を変更するかどうかを指定する。保存先を変更する場合は、分割鍵保有者は、保存先を直接入力するか、または図23中の下段の「参照」ボタン2301をクリックする。保存先を変更しない場合は、ステップ1811へ進む。

【0148】ステップ1809で分割鍵保有者が「参照」ボタン2301をクリックすると、ステップ1810において、中央処理部1501は、表示部1503に保存先参照画面を表示する。図24は、保存先参照画面の表示例である。

【0149】保存先参照画面が表示されると、分割鍵保有者は、前記保存先参照画面からファイル復号後の保存先を入力する。保存先が入力されると、中央処理部1501は、表示部1503にファイル・保存先入力画面を再び表示する。保存先が決まると、ステップ1811において、分割鍵保有者は、図23中の「回復」ボタンをクリックする。

【0150】分割鍵保有者が「回復」ボタンをクリックすると、中央処理部1501は、ファイル復号部1506に対して、入力されたファイルの復号処理を依頼する。ファイルが復号されると、中央処理部1501は、入力された保存先に復号されたファイルを保存する。ファイル復号処理の詳細は図26で説明する。

【0151】ファイルが保存されると、ステップ1812において、中央処理部1501は、表示部1503に終了画面を表示する。図25は、終了画面の表示例である。復号したファイルの所有者「ryoko」と名前「C:\temp\暗号readme. txt」が表示されている。終了画面が表示されると、分割鍵保有者は、図25中の「OK」ボタンをクリックしてファイル復号処理を終了する。

【0152】本発明の実施形態には、以上に説明したもの他に様々なバリエーションが考えられる。以下、図18のファイル復号フロー図の復号の変更という形で、前記バリエーションについて説明する。

【0153】まず、ステップ1803～1805の分割鍵保有者認証と、1806～1810のファイル・保存先入力の手順とは、互いに入れ換えることが可能である。また、ステップ1811でファイルを復号した後、図25の終了画面の代わりにファイルオープン選択画面を表示して、分割鍵保有者がファイルオープンを選択した場合には、前記ファイルに関連付けられたアプリケーションプログラムを起動して、前記アプリケーションから復号したファイルを開くようにしてもよい。

【0154】図27は、ファイルオープン選択画面の表示例である。復号したファイルの所有者と名前が表示されている。

【0155】分割鍵保有者は、復号したファイルを開く場合は図27中の「はい」ボタンを、開かない場合は図27中の「いいえ」ボタンをクリックする。分割鍵保有者が「はい」ボタンをクリックした場合は、ファイルに関連アプリケーションで開く。図27に示した例では、復号したファイルはテキストファイルであるので、この場合は通常テキストエディタが起動して前記ファイルが開くことになる。

【0156】本実施形態では、復号するファイルの数は1個だけであったが、ステップ1806において、分割鍵保有者がファイルを複数入力できるようにして、複数のファイルの復号できるようにしてもよい。この場合、各ファイルの復号後の保存先のディレクトリを同じにしてもよいし、ファイルごとに別々にしてもよい。

【0157】また、前記ファイルの複数入力をさらに発展させて、ステップ1806で分割鍵保有者がディレクトリを指定できるようにして、前記ディレクトリに属するすべてのファイルを一度に復号できるようにしてもよい。

【0158】本実施形態では、ファイル復号部（ファイル復号プログラム）1506を起動してから復号するファイルを選択していたが、例えばファイラーから予め復号したいファイルを選んでおき、マウスの右ボタンをクリックするなどの方法でポップアップメニューを表示し、前記ポップアップメニューからファイル復号部1506を起動するといった方法もある。

【0159】分割鍵保有者がファイルの内容を確認したいたけならば、復号したファイルを必ずしもどこかに保存する必要はない。復号したファイルをテンポラリファイルとしておき、関連アプリケーション起動後に前記テンポラリファイルを開き、前記アプリケーションを終了すると前記テンポラリファイルが消去されるようにしてもよい。

【0160】ファイル復号部1506を、復号したいフ

ファイルがある利用者計算機から起動する必要もない。復号したいファイルがある利用者計算機から、前記ファイルの C_1 、 C_2 などのファイル復号に必要な情報を取り出して、フロッピーディスクなどの持ち運び可能な媒体に格納し、分割鍵保有者の計算機などの他の計算機からファイル復号部1506を起動して、前記媒体内の情報からファイルを復号させてもよい。以上に説明したバリエーションを複数組み合わせるといったことも可能である。

【0161】図26を用いて、暗号化したファイルをファイル復号部1506にて復号する手順について説明する。まず、ステップ2601において、図7のステップ701と同様にして、復号したい文書と対応する C_1 と C_2 とをファイル暗号部1504から取り出す。次に、ステップ2602において、各 S_j を中央処理部1501から取り出す。続くステップ2603において、各 D_j を次の、数37によって計算する。

【数162】

【数37】

【数37】

$$D_j = C_j^{S_j}$$

【0163】本実施形態では、ファイル復号処理はすべて同一の利用者計算機上で行っている。このため、ステップ2602、2603では、図7と異なり、各 S_j から D_j を直接計算している。

【0164】次に、ステップ2604において、図7のステップ705と同様にして平文Mを求める。

【0165】

【数38】

【数38】

$$M = C/\prod D_j^{27w}$$

【0166】次に、ステップ2605において、平文Mを使って、暗号化した文書を復号する。なお、上記各実施形態において、各計算機が実行する処理は、CD-ROM等の記録媒体に記録して各計算機にインストールして実行するように構成することができる。あるいは、記録媒体に代えて、インターネット等の通信媒体を用いて各計算機にインストールして実行させることができる。

【0167】また、本発明の適用範囲である鍵の分割は個人単位に限定されるものではなく、団体、グループを対象としても構わない。

【0168】

【発明の効果】以上の説明から明らかなように、本発明によれば、暗号文を復号する際には秘密鍵そのものはどこにも復元されず、分割鍵保有者計算機が持つ分割鍵 S_j に基づいて部分的に復号したデータ D_j を使って必要な文書を復号しているため、同じ鍵を用いて、暗号化した他の文書を復号することはできない。

【0169】また、秘密鍵自体が知られることもない。そして、複数人の分割鍵保有者の協力により、公開鍵で

暗号化されたデータを目的とする暗号文のみに限って復号することができ、かつその分割鍵の管理も容易である。

【0170】供託機関に供託した鍵を用いるようにした場合、1人のユーザに対して1つの分割鍵を持っており、従来技術としてあげたMicaliの方法のように1人に対して複数の分割鍵を保管する必要があるため、保管のコストを下げるができる。

【0171】したがって、例えば、企業内で担当者が作成、暗号化した文書を、その担当者がいない時に復号する必要がある場合、担当者の上長や所属のコンピュータ管理者が協力して復号する場合に好適である。

【0172】また、公開鍵暗号の秘密鍵供託方式において、特に複数の供託機関に秘密鍵を分割して供託する場合にも好適である。

【0173】さらに、分割鍵保有者をグループ化することにより、復号の際には上位の権限を持つ分割鍵保有者の参加を必ず必要とする運用が可能となる。

【0174】さらに、分割鍵保有者をグループ化することにより、保有者変更時の分割鍵再配布の範囲を狭くしたり、復号の際には上位の権限を持つ分割鍵保有者の参加を必ず必要としたりする、柔軟な運用が可能となる。

【0175】さらに、本発明のデータ復号インタフェースを用いれば、分割鍵保有者が暗号ファイルを容易に復号することができるので、担当者不在時の問い合わせにも、前記担当者所有の暗号ファイルを復号して内容を確認することで対応できる。また、前記担当者がパスワードを忘れた場合にも対応できる。

【図面の簡単な説明】

【図1】本発明を適用した暗号データの復号システムの一実施形態を示すシステム構成図である。

【図2】システム構築時に行う処理の概要を示すフローチャートである。

【図3】恒等式 T_1 の生成方法を示すフローチャートである。

【図4】鍵生成装置に行う利用者の登録方法を示すフローチャートである。

【図5】利用者計算機を用いて、自分が作成した文書を暗号化する手順を示すフローチャートである。

【図6】利用者計算機を用いて暗号化した文書を復号する手順を示すフローチャートである。

【図7】暗号化した文書をデータ復号装置にて復号する手順を示すフローチャートである。

【図8】図7までの処理全体を分かり易くまとめた説明図である。

【図9】本発明を鍵供託に用いた場合の復号方法の説明図である。

【図10】本発明の第2の実施形態において、システム構築時に行う処理の概要を示すフローチャートである。

【図11】第2の実施形態における恒等式 T_1 の生成方

法を示すフローチャートである。

【図 1 2】第 2 の実施形態における鍵生成装置にて行う利用者の登録方法を示すフローチャートである。

【図 1 3】第 2 の実施形態における利用者計算機を用いて、自分が作成した文書を暗号化する手順を示すフローチャートである。

【図 1 4】秘密鍵のグループ分割の仕方の例を示す図である。

【図 1 5】本発明の第 3 の実施形態を示すシステム構成図である。

【図 1 6】第 3 の実施形態において、システム構築時に扱う処理の概要を示すフローチャートである。

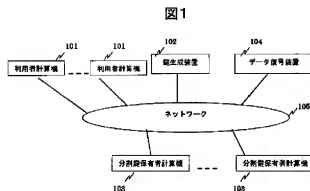
【図 1 7】第 3 の実施形態における利用者の登録方法を示すフローチャートである。

【図 1 8】第 3 の実施形態において、利用者計算機を用いて暗号化された文書を分割鍵保有者の鍵を用いて復号する手順を示すフローチャートである。

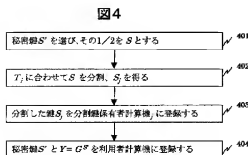
【図 1 9】第 3 の実施形態において表示部に表示されるファイル回復情報画面の例を示す図である。

【図 2 0】第 3 の実施形態において表示部に表示される

【図 1】



【図 4】



管理者認証画面の例を示す図である。

【図 2 1】第 3 の実施形態において表示部に表示されるファイル・保存先入力画面の例を示す図である。

【図 2 2】第 3 の実施形態において表示部に表示されるファイル参照画面の例を示す図である。

【図 2 3】第 3 の実施形態において表示部に表示されるファイル・保存先入力画面の例を示す図である。

【図 2 4】第 3 の実施形態において表示部に表示される保存先参照画面の例を示す図である。

【図 2 5】第 3 の実施形態において表示部に表示されるデータ復号終了画面の例を示す図である。

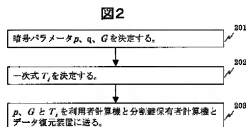
【図 2 6】第 3 の実施形態においてデータの復号手順の詳細を示すフローチャートである。

【図 2 7】第 3 の実施形態において表示部に表示されるファイルオープン選択画面の例を示す図である。

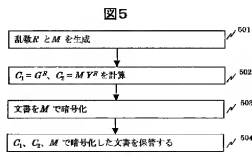
【符号の説明】

1 0 1 …利用者計算機、1 0 2 …鍵生成装置、1 0 3 …分割鍵保有者計算機、1 0 4 …データ復号装置、1 0 5 …ネットワーク、1 1 2-1 ~ 1 1 2-N …供託機関計算機。

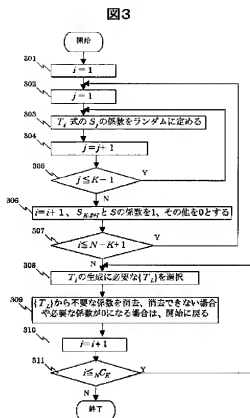
【図 2】



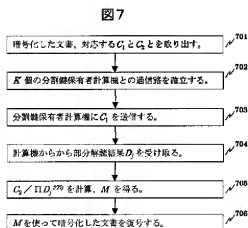
【図 5】



【図3】



【図7】



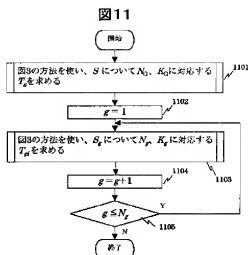
【図19】



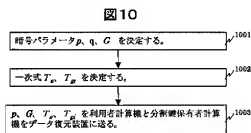
【図6】



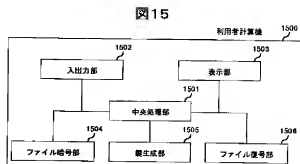
【図11】



【図10】



【図15】



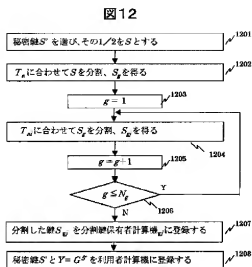
【図8】



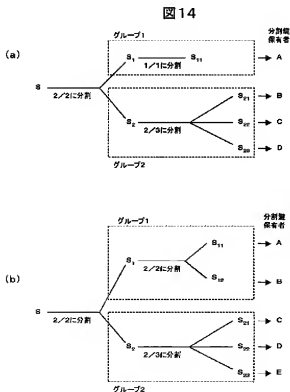
【図 9】



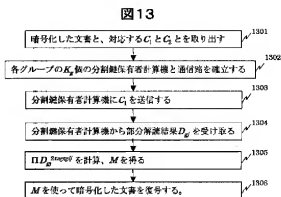
【図12】



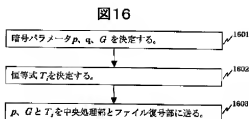
【図14】



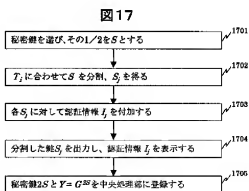
【図13】



【図16】



【図17】



【図20】



【図18】

図18

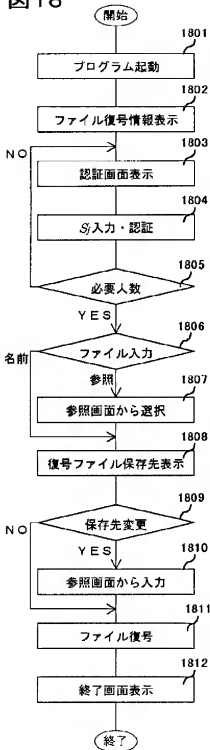


図21



【図22】

図22



【図23】

図23



【図24】

図24



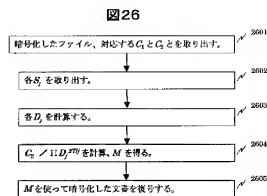
【図25】



【図27】



【図26】



フロントページの続き

(72)発明者 宮崎 博
 神奈川県横浜市中央区尾上町6丁目81番地
 日立ソフトウェアエンジニアリング株式会
 社内

(72)発明者 遠田 満一
 神奈川県横浜市中央区尾上町6丁目81番地
 日立ソフトウェアエンジニアリング株式会
 社内